



# HOW TO MEET **DATA BACKUP AND RECOVERY NEEDS** WITH LIMITED RESOURCES

# TABLE OF CONTENTS

1. Facing SMB backup challenges
2. Problem: Regulatory compliance
3. Problem: Identifying backup data
4. Problem: Cheapest is not always best
5. Problem: Tackling what-if scenarios
6. Problem: 'Set it and forget it' mentality
7. Problem: Lack of backup expertise
8. Solution: Learn from the data-protection specialists



# CHALLENGES

FACING SMB BACKUP  
CHALLENGES



Businesses typically have a lot of pressure to generate a profit while operating at maximum efficiency. This pressure is increased tenfold for small and medium-sized businesses. These entities have to deal with limited budgets, resources and staff, all while operating

effectively and delivering quality services to their customers. Think of firms like the local doctor or dentist, law offices, CPAs or manufacturing and construction companies. Many of these businesses rely on their internal experience to keep everything running without breaking the bank.



One area these organizations have in common is the need for data backup and recovery. As technology advances and businesses evolve, so too do modern threats. Accidental and malicious behavior resulting in data loss has become an increasingly likely occurrence. This leaves SMBs often struggling to maintain data security with limited internal IT resources. However, when handling these complexities without the support of experts, businesses open themselves up to numerous potential issues. Backups that overlook new sources of data could ruin their chances of restoring critical assets in an emergency. A poorly constructed retention policy could affect an organization's compliance with privacy regulations.

Let's take a look at some of the most common problems SMBs experience with meeting their data backup and recovery needs and discuss how to manage these requirements using every resource at their disposal.





# PROBLEM #1

PROBLEM:  
REGULATORY  
COMPLIANCE



Nearly every industry has a set of established standards that businesses must follow to secure data and remain operational. All health care institutions have to comply with the Health Insurance Portability and Accountability Act, for example, which sets guidelines for protecting patient information. Any business that handles payment card data must adhere to the Payment Card Industry Data Security Standard. However, due to the broad reach, and complicated and often vague provisions of HIPAA, many businesses feel alone without the proper guidance to meet the security requirements needed for compliance. Often HIPAA laws don't specifically say how to do things, they simply provide guidelines for what needs to be accomplished.



With these laws in place, it's hard to gauge how to be 100 percent compliant, and these standards are being enforced more aggressively. Organizations are being fined for breaches of patient information and financial data. Just look at the Anthem breach, which affected 80 million people.

After the incident, Anthem provided credit monitoring, took a huge hit to its reputation and ended up spending over \$100 million to recover. SMBs must consider data retention, how long you need to keep data and how much space is available.

To further complicate matters, state laws govern how long medical records must be retained, so the requirements for each state will differ. In some states, medical and dental records for patient data must be kept for at least 7 years from the last date of treatment, and when it comes to minors, some states require everything to be retained for an additional two or three years after that patient reaches the age of 18. This all falls under compliance, and it will be critical to know what must be stored as well as how to protect it.





# PROBLEM #2

PROBLEM:  
IDENTIFYING  
BACKUP DATA



Another issue is that many SMBs don't know how to determine what data they actually need to retain. What happens if you've lost a particular folder? Is it something you can recreate? How long will you be down or what will be the cost if a production server is not recoverable? Is it worth investing in backup to ensure minimal downtime? You need to weigh the risks of downtime versus the cost of implementing a comprehensive recovery system.

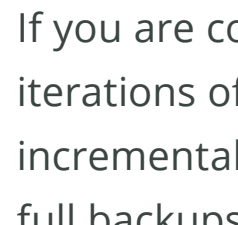


Many organizations end up backing up everything because they don't know what to back up. This is better than doing nothing. But as you build your business plan for data protection, it will be important to understand the options available to you, including understanding the difference between an image backup and a file backup.

With image-level backups, you can back up assets like your operating system, and applications by taking a snapshot of the entire system. File-level backups just address files on your system.

You'll likely want to do an image backup once a month or when any major changes are made to applications and operating systems. It's also recommended to conduct a full file backup of all critical files weekly, and do a daily differential, which includes all changes made since the last full backup.





If you are concerned about keeping iterations of your data, daily incremental backups done between full backups will allow you to roll-back to previous versions of your data. While incremental backups offer greater flexibility when it comes to recovery, they are also known for taking longer to restore as each incremental must be restored consecutively following the recovery of your full backup. Differentials offer an advantage in this area, in that just the full and the latest differential backup has to be restored to get back up and running if you run into a disaster scenario.

It's important to understand what is more important to your business, the ability to recover quickly, or the ability to recover iterations of your data. While there are other considerations like how much data you are trying to backup and how much storage capacity you have, you need to know what your options are, so you can make an educated decision based on your business needs. Over time your needs may change depending on the amount of data, storage and the importance of the data you are looking to protect.





# PROBLEM #3

PROBLEM:  
CHEAPEST IS NOT  
ALWAYS BEST



Another big mistake is choosing the cheapest backup option simply because you need some sort of recovery solution. This often involves online services and providers that don't give much support. If you lose your data, it might take them hours, days or weeks to get that information back depending on how much data it is and how strong your Internet connection may be. If you don't have a local backup, you need to consider how long it will take to retrieve your assets via the cloud.




Most SMBs operate under tight budgets and a lack of hardware resources, so your solution has to be flexible enough to work with consumer-grade media. It's also important to note that if you're using freeware, you may not have the technical support you desire when it comes time to restore.

For instance, Microsoft offers a built-in solution, but it can be difficult trying to call them for help. Knowing that you have a backup expert in your corner is huge.

On a day-to-day basis, it may be hard to see the value of selecting the right backup solution, when in reality it could be critical to the future of your business and selecting the cheapest option is not always what's best for your success.





Does your solution offer license flexibility? Perhaps you'd prefer a perpetual license purchased via an authorized reseller, or alternately an affordable monthly subscription plan – always kept up-to-date with the latest technology. Your backup solution should offer cloud storage options that match both the size of your data and your budget. Those who'd like to manage their data protection centrally must have a program available as an option for future growth.





# PROBLEM #4

PROBLEM: TACKLING  
WHAT-IF SCENARIOS



It's hard to come to terms with questions like "What if my business is hacked?" or "What if the servers are compromised due to flooding?" You may have everything all set to overwrite, using a single drive that's ready to backup to every day. But what if that drive dies, becomes corrupted or virus-infected, or you unintentionally overwrote your only backup? These types of situations commonly occur and it's better to prepare for them now than to simply hope it never happens.



Your recovery strategy should include having a backup of your backup, rotating the media that you're backing up to regularly and storing an additional copy off-site.

The easiest way to do this is to follow the 3-2-1 rule: three backup copies, using two different types of media, with one stored off-site. This method will help ensure that you always have your backups ready when you need them most.

You could for example backup your files locally to a server, and also use two network-attached storage devices that have NAS replication, to just run the backup once and automatically duplicate the backups to multiple pieces of hardware. One device could be stored on-site and one off-site. You could also use a cloud backup as your off-site backup, just make sure you also have your local backups in place. Whatever method you decide on, you need to ensure accessibility and that your backup plan will meet your needs during various "what-if" scenarios.



# PROBLEM #5

PROBLEM:  
LACK OF  
BACKUP EXPERTISE



Your best backup solution for your business will be a configurable, flexible piece of software with the features that allow you to protect your data the way that you want. However, with so many options available to you, it may leave room for error for less technical employees. There's always the chance of backup jobs not being set up right to begin with. Because it is complex, it is often helpful to have someone guide you through the setup of initial backup jobs.



Without an IT team, who would create the initial backup? Would the owner, the receptionist or someone else take on the challenge? Likely this person has limited IT knowledge or they may not know what data is most critical to the business at large. They also may not understand how to best protect the business from complicated malware like CryptoLocker and other threats.

Your business requires a solution, which can be customized and set up to meet your specific business needs. Often, consulting with an expert at the time of installation can ensure that your business gets the most out of their backup solution.



Your recovery strategy should include having a backup of your backup, rotating the media that you're backing up to regularly and storing an additional copy off-site.

The easiest way to do this is to follow the 3-2-1 rule: three backup copies, using two different types of media, with one stored off-site. This method will help ensure that you always have your backups ready when you need them most.

You could for example backup your files locally to a server, and also use two network-attached storage devices that have NAS replication, to just run the backup once and automatically duplicate the backups to multiple pieces of hardware. One device could be stored on-site and one off-site. You could also use a cloud backup as your off-site backup, just make sure you also have your local backups in place. Whatever method you decide on, you need to ensure accessibility and that your backup plan will meet your needs during various "what-if" scenarios.





SOLUTION: LEARN FROM  
THE DATA-PROTECTION  
SPECIALISTS

THE SOLUTION



All the solutions to these problems can be resolved by consulting NovaBACKUP or one of our certified reseller partners. We have backup experts and resellers on-call to help you configure your backups to your specific requirements. Utilize NovaBACKUP's setup assistance with a backup engineer who understands your business or partner with a reseller who can walk you through everything step by step. Many of our partners cater to specific industries and will be able to offer detailed insights to those sectors. With the help of a local partner, you can work side by side with an expert to make sure your backup solution is configured on-site and addresses best practices for your industry. NovaBACKUP partners have direct access to NovaBACKUP technical support so you always get the assistance you need.



We understand that SMBs have a lot on their plate and may not be able to rely on internal IT for data backup and recovery needs.

However, by teaming up with NovaBACKUP and our partners, you can tackle tough issues such as lack of IT experience, compliance requirements, what-if scenarios and determining what data should be part of your backups without an IT team and without breaking the bank.

To find out more about boosting your backup and recovery capabilities, contact NovaBACKUP or one of our certified reseller partners today!





NovaBACKUP Corporation  
29209 Canwood St.  
Agoura Hills, CA 91301, USA

Tel: +1.805.579.6700  
[ols@novabackup.com](mailto:ols@novabackup.com)

NovaBACKUP GmbH  
Marienstrasse 89, 30171 Hannover,  
Deutschland

Tel: +49 40 80811371  
[kontakt@novabackup.com](mailto:kontakt@novabackup.com)

NovaBACKUP's team of data-protection experts are a dedicated technical resource for all of your backup related questions. As an extension of your IT staff, we're here to help you make informed technology decisions. Schedule a consultation today for an evaluation of your environment.